An inductive proof of fundamental theorem of arithmetic.

Kevin Buzzard

February 7, 2012

Last modified 07/02/2012.

In the first term of a mathematical undergraduate's education, he or she might typically be exposed to the standard proof of the fundamental theorem of arithmetic, that every positive integer is uniquely the product of primes. The standard proof goes as follows. Firstly, existence of a prime decomposition is immediate by induction. Then one establishes the validity of Euclid's algorithm, and deduces that if a, b are positive integers then there exists $\lambda, \mu \in \mathbf{Z}$ such that $\lambda a + \mu b = \gcd(a, b)$, the greatest common divisor of a and b. One uses this key intermediate result to prove that if a prime divides the product of two integers, then it divides at least one of the integers. And now it's all downhill; uniqueness of prime factorization follows without too much difficulty by induction.

In practice, this is a pain to lecture. The problem is that to explain Euclid's algorithm to 200 first years one has to make sure one has prepared sufficiently well enough to make the notation used both correct and sensible; one has quotients q_i and remainders r_i and one has to be careful about "off-by-one" errors in the indices; proving that Euclid's algorithm spits out the greatest common divisor also needs to be done, and this involves checking firstly that the algorithm spits out a common divisor and secondly that it's the greatest one; both of these are consequences of a simple induction, as long as you, in both cases, manage to correctly formulate the statement that you need to prove by induction! One can take a good half-hour setting all of this up, and this is just Euclid's algorithm; there is still half an hour more of material before one finally gets to the proof of the fundamental theorem.

Recently I came across an article (note added 2012: AARGH! I never wrote down the reference when I wrote this in 2006! But is this proof in Davenport's book as well?) that gave a simple proof of uniqueness of prime factorization, by induction. I was so incredulous that I dismissed the argument as incorrect after a cursory read, and it was only after the ramifications of the trick began to sink in that I began to believe that the argument could possibly work. I am still a little bewildered by it. I have mentioned it to several people and none of them appeared to know the argument either. I present it here.

Theorem 0.1. *Every positive integer is uniquely, up to re-ordering, the product*

of primes.

Proof. By induction. Note that the existence of a prime factorization of a positive integer is trivial (also by induction) so all we have to do is to check uniqueness. It's true for $n = 1$ (the empty product is the only possibility, as every non-empty product of primes is greater than 1) so let's assume $n > 1$ and that every integer between 1 and $n-1$ is uniquely the product of primes. Let's write $n = p_1 p_2 \dots p_r = q_1 q_2 \dots q_s$ with the p_i and q_j prime. Note that $n > 1$ so certainly $r, s \geq 1$. All we have to do is to check that p_1 is one of the q_j and then we are home by the inductive hypothesis (cancel $p_1 = q_j$ and what is left is uniquely the product of primes so all the other p's and q's must match up). If $p_1 = q_1$ then we are done. If not then WLOG $p_1 < q_1$. Now choose a prime factorization of $q_1 - p_1$:

$$q_1 - p_1 = r_1 r_2 \dots r_t$$

with the r_k prime and $t \geq 0$, and now consider the integer

$$\begin{aligned} m := r_1 r_2 \dots r_t q_2 q_3 \dots q_s &= (q_1 - p_1) q_2 q_3 \dots q_s \\ &= n - p_1 q_2 q_3 \dots q_s. \end{aligned}$$

Then $0 < m \leq n - p_1 < n$ and hence by the inductive hypothesis, m is uniquely the product of primes. The killer observation is that p_1 divides both n and $p_1 q_2 q_3 \dots q_s$, and hence p_1 divides their difference, which is m. We may write m/p_1 as a product of primes, and we deduce that m has a prime factorization which mentions p_1. By uniqueness, we deduce that either p_1 is one of the r_k or one of the q_j, $j \geq 2$.

If $p_1 = q_j$ for some $j \geq 2$ then we are home. So let us assume that p_1 is one of the r_k. Then p_1 divides $q_1 - p_1$ and hence p_1 divides q_1. But this is a contradiction because $1 < p_1 < q_1$ and q_1 is prime. □

References

[1] ?